Dr. Eberhard Manz
GM 2238 PCT

Patent Claims

1. Method for proving the pedigree and/or for the identification of animals or of biological material from animals and organisms, which comprises the following steps:
   - storing on a data carrier identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological material,
   - verifying the identification data with respect to whether said data have the predetermined connection with the genetic information.

2. Method according to Claim 1, [lacuna] that the genetic information of one or more animals or of biological material from one or more animals or organisms is determined and is stored as reference datasets on a storage medium.

3. Method according to Claim 1 or 2, characterized in that the data carrier holds further data which have been assigned to the identification data and which relate to the animal to be identified or the biological material to be identified.

4. Method according to Claim [sic] 1 to 3, characterized in that the identification data contain an encrypted message which has been encrypted using a code unambiguously assigned to the individual animal or material.

5. Method according to Claim 4, characterized in that the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be identified or the biological material to be identified.

6. Method according to one [lacuna] Claims 1 to 5, characterized in that an encrypted message comprises genetic information unambiguously identifying the animal or the material.

7. Method according to one of Claims 3 to 6, characterized in that the identification data comprise encrypted data which relate to the storage location and/or the contents of further data which relate to the animal assigned to the identification data.

8. Method according to one of Claims 4 to 7, characterized in that the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

9. Method according to Claim 8, characterized in that the sequence of digits forms at least part of the code.

10. Method according to Claim 8 or 9, characterized in that the key is a symmetric key.

11. Method according to Claim 8 or 9, characterized in

that the message has been encrypted on the basis of the private key of an asymmetric pair of keys, with the public key at least in part having a predetermined connection with the genetic information identifying the animal or the material.

12. Method according to Claim 11, [lacuna] that the public key comprises a part specific for the animal or the material and a user-specific part.

13. Method according to one of Claims 8 to 12, characterized in that the identification data are additionally encrypted using a user-specific key.

14. Method according to one of Claims 8 to 13, characterized in that the data on the data carrier, which have been assigned to the identification data, have at least in part been encrypted by a code which is different than the code used for encrypting the identification data.

15. Method according to one of Claims 8 to 14, characterized in that the key for decrypting the message contained in the identification data is stored on a carrier of a chip for communicating with a data processing system via an interface, in particular on a smartcard.

16. Method according to Claim 15, characterized in that the chip has a device for decrypting messages.

17. Method according to Claim 15 or 16, characterized in that the key encoding the message of the identification data is an asymmetric key, the corresponding private key is stored on the chip and the chip has a device for encrypting messages using

the private key.

18. Method according to one of Claims 15 to 17, characterized in that the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

19. Method according to Claims 18, characterized in that the comparing device compares the entered digitized genetic information with a stored value for this information and emits an output signal which indicates whether or not there is a match.

al cont

20. Method according to Claim 18, characterized in that, based on the entered digitized genetic information and a stored assignment to the stored key of digitized genetic information unambiguously identifying the animal or the material, the comparing device determines a key assigned to the entered information, compares the key determined in this way with the stored key and releases an output signal which indicates whether or not the key determined based on the input matches the stored key.

21. Method according to one of Claims 15 to 20, characterized in that the chip holds information identifying one or more users and the decrypting device or encrypting device is only activated when information stored for identifying a user is entered via an input device.

22. Method according to one of Claims 8 to 21, characterized in that the code for decrypting coded information contained in the identification data is stored on a central computer.

23. Method according to Claim 22, characterized in that the computer determines the corresponding key owing to entered or predetermined genetic information and applies said key to the identification data.

24. Method according to Claim 23, characterized in that, after decrypting, the central computer verifies whether predetermined sequences of characters are present in the decrypted text and releases a corresponding output signal to a user.

25. Method according to Claim 23 or 24, characterized and that the information stored on the data carrier and, where appropriate, predetermined genetic information unambiguously identifying the animal or the material are transferred to the central computer.

26. Method according to one of Claims 1 to 24, characterized in that the data carrier containing the data related to the animal or the material is stored on a central computer.

27. Method according to Claim 26, characterized in that at least in part the data are access-protected and that access authorization is different for different users of the central computer.

28. Method according to Claim 27, characterized in that a proportion of users can access at least part of the stored data only, if a predetermined further user is logged on to the central computer at the same time.

29. Method according to one of Claims 26 to 28, characterized in that access to at least part of the stored data is only possible, if the computer has

verified access authorization using the data stored on a chip, in particular on a smartcard.

30. Method according to one of Claims 27 to 29, characterized in that the computer is set up such that users can write to the stored data related to the animal or the material only together with a digital signature of the user.

31. Method according to one of Claims 26 to 30, characterized in that an animal-specific pair of asymmetric keys is used for exchanging a session key for communication of a user with the central computer.

32. Method for generating data which are unambiguously and verifiably connected with an individual animal, which comprises:

- creating identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information which unambiguously identifies an animal or the biological material.
- storing the identification data on a data carrier.

33. Method according to Claim 32, characterized in that the identification data contain an encrypted message which has been encrypted using a key unambiguously assigned to the individual animal.

34. Method according to Claim 33, characterized in that the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to

the animal to be identified or the biological material to be identified.

35. Method according to one of Claims 32 to 34, characterized in that the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

36. Method according to Claim 35, characterized in that the key is a symmetric key.

G2 cont

37. Method according to Claim 35, characterized in that the information has been encrypted on the basis of an asymmetric pair of keys, with the public key at least in part having a predetermined connection with the genetic information.

38. Chip carrier for identifying animals, which is set up for communication between a chip on the chip carrier and a computer via an interface, in particular a smartcard, characterized in that the chip holds a key which has an unambiguous and predetermined connection with genetic information specific for the individual animal.

39. Chip carrier according to Claim 38, characterized in that the chip has a processor for decrypting messages using the stored key.

40. Smartcard according to one of Claims 38 or 39 [sic], characterized in that the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored

code to entered digitized genetic information.

41. Computer system for carrying out a method according to one of Claims 1 to 31, characterized by a central computer having a data carrier which holds identification data which have an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological material.